UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/805,017	03/18/2004	Wilson Sing-Hei So	36992.00107 (HAL 265)	7773

44955 7590 11/15/2007

SQUIRE, SANDERS & DEMPSEY L.L.P.
1 MARITIME PLAZA, SUITE 300
SAN FRANCISCO, CA 94111

EXAMINER	
JOHNS, CHRISTOPHER C	
ART UNIT	**PAPER NUMBER**
4172	
MAIL DATE	**DELIVERY MODE**
11/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/805,017	SO ET AL.	
	Examiner	Art Unit	
	Christopher C. Johns	4172	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/18/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 20 rejected under 35 U.S.C. 101 because it is drawn to functional descriptive material that is not embodied on a computer-readable medium. See MPEP §2106.01.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 3-6, 8-12, 14-16, and 18-20 rejected under 35 U.S.C. 102(b) as being anticipated by US Patent 6,105,008 (hereafter referred to as Davis et al).

As per claim 1:

Davis et al teaches:

- a first site coupled to a network, a terminal coupled to the network for performing a first portion of a transaction with the first site via the network…a secure device coupled to the terminal (cf. Figure 10 – the smart card is used on a computer; cf. Abstract – "for payment of goods and/or services purchased on-line over the Internet"),

- the secure device containing an encrypted version of the personal data and a first key for decrypting the encrypted personal data, wherein the secure device provides the terminal with the encrypted personal data and the first key to the terminal (cf. column 19, lines 52-67)
- the terminal having logic for decrypting the encrypted personal data using the first key, logic for re-encrypting the decrypted personal data with a second key, and logic for transmitting the re-encrypted personal data to the second site via the network (In using the Internet to effect transactions, it is inherent for the terminal to decrypt the smartcard data in order to read it, and then to re-encrypt it using an encryption protocol that the destination would understand. A terminal would need to be able to read the information from the smart card and would so decrypt it. In order to send the information over the Internet, it must be encrypted for security purposes),
- the second site having logic for decrypting the re-encrypted personal data and logic for using the personal data to complete the second portion of the transaction (cf. column 20, lines 1-19).

As per claim 3:

Davis et al discloses:

- communications between the terminal and the secure device and between the terminal and the second site are encrypted with one or more symmetric keys (cf. column 19, lines 52-67)

As per claim 4:

Davis et al discloses:

- the personal data includes at least one of credit card information and credit history information (cf. Abstract – the smart card can be used "for payment of goods and/or services purchased on-line over the Internet"; column 1, lines 30-35).

As per claim 5:

Davis et al discloses:

- list containing information for authenticating the certificate of the second site is transmitted from the first site to the terminal via the network prior to receipt of the certificate by the terminal (cf. Figure 11A, step 606; this allows the client terminal to understand where to go for payment (because part of the information sent is the IP address of the payment server) as well as identifies the transaction and the merchant using identifiers (allowing for further verification of the validity of the server).

As per claim 6:

Davis et al discloses:

- transaction comprises a commercial transaction and the first site comprises an e-commerce site (cf. Abstract, "uses a smart card for payment of goods and/or services purchased on-line over the Internet")

As per claim 8:

Davis et al discloses:

- second key comprises a public key associated with the second site (cf. column 19, lines 52-67).

As per claim 9:

Davis et al discloses:

- second certificate associated with the terminal is provided to the secure device to authenticate the terminal before the secure device provides the terminal with the encrypted personal data and first key (cf. column 7, line 65, to column 8, line 10)

As per claim 10:

Davis et al discloses:

- notification is transmitted from the second site to the first site via the network upon completion of the second portion of the transaction (cf. Figure 11C, steps 634, 636, 638, 640).

As per claim 11:

Davis et al discloses:

- secure device is detachably coupled to the terminal (cf., for example, Figure 4 – the smart card is inside a Card Reader. This is inherent in the definition of a smart card).

As per claim 12:

Davis et al discloses:

- receiving, via a network, a request from a site to perform a portion of a transaction with a terminal coupled to the network, wherein an initial portion of the transaction is performed between the site and the terminal via the network,

wherein personal data about a user of the terminal is required to complete the requested portion of the transaction (Figure 10 teaches using the smart card on a computer, to enable an Internet purchase with a merchant website),

- transmitting a certificate to the terminal via the network, wherein the terminal authenticates the certificate and transmits via the network an indication that indicates that the certificate has been authenticated, transmitting a request for the personal data to the terminal via the network, wherein a secure device is coupled to the terminal (cf. column 19, lines 52-67, and Figure 10; the secure device in Davis et al uses a variety of encryption techniques to prevent loss of personal information, all of which are inherent to the art of online purchases and transactions)
- wherein the secure device contains an encrypted version of the personal data and a first key for decrypting the encrypted personal data, wherein the secure device provides the terminal with the encrypted personal data and the first key and the terminal uses the first key to decrypt the encrypted personal data; providing the terminal with a second key via the network (cf. column 19, lines 52-67),
- wherein the terminal re-encrypts the personal data with the second key; receiving the re-encrypted personal data from the terminal via the network; decrypting the re-encrypted personal data with the second key; and completing the requested portion of the transaction using the personal data (In using the Internet to effect transactions, it is inherent for the terminal to decrypt the smartcard data in order

to read it, and then to re-encrypt it using an encryption protocol that the destination would understand. A terminal would need to be able to read the information from the smart card and would so decrypt it. In order to send the information over the Internet, it must be encrypted for security purposes).

As per claim 14:

Davis et al discloses:

- communications with the secure device and the terminal are encrypted with one or more symmetric keys (cf. column 19, lines 52-67).

As per claim 15:

Davis et al discloses:

- the personal data includes at least one of credit card information and credit history information (cf. Abstract – the smart card can be used "for payment of goods and/or services purchased on-line over the Internet"; column 1, lines 30-35).

As per claim 16:

Davis et al discloses:

- prior to transmission of the certificate to the terminal, the site transmits to the terminal via the network a list containing information for authenticating the certificate (cf. Figure 11A, step 606; this allows the client terminal to understand where to go for payment (because part of the information sent is the IP address of the payment server) as well as identifies the transaction and the merchant using identifiers (allowing for further verification of the validity of the server).

As per claim 18:

Davis et al discloses:

- second certificate associated with the terminal is provided to the secure device to authenticate the terminal before the secure device provides the terminal with the encrypted personal data and first key (cf. column 7, line 65, to column 8, line 10)

As per claim 19:

Davis et al discloses:

- notifying the site via the network of the completion of the requested portion of the transaction (cf. Figure 11C, steps 634, 636, 638, 640).

As per claim 20:

Davis et al discloses:

- performing a first portion of transaction with a first site via a network, wherein the first site contacts a second site via the network to request that the second site perform a second portion of the transaction, wherein personal data about a user is required to complete the second portion of the transaction (Figure 10 teaches using the smart card on a computer, to enable an Internet purchase with a merchant website),
- computer code for receiving a certificate from the second site via the network; computer code for authenticating the certificate of the second site; computer code for contacting the second site via the network if the certificate is authenticated; computer code for receiving a request for the personal data from the second site via the network (cf. column 19, lines 52-67, and Figure 10; the

secure device in Davis et al uses a variety of encryption techniques to prevent loss of personal information, all of which are inherent to the art of online purchases and transactions")

- wherein the secure device contains an encrypted version of the personal data and a first key for decrypting the encrypted personal data, wherein the secure device provides the terminal with the encrypted personal data and the first key and the terminal uses the first key to decrypt the encrypted personal data; providing the terminal with a second key via the network (cf. column 19, lines 52-67),
- computer code for requesting the personal data from a secure device, wherein the secure device contains an encrypted version of the personal data and a first key for decrypting the encrypted personal data; computer code for receiving the encrypted personal data and the first key from the secure device; computer code for decrypting the encrypted personal data using the first key; computer code for re-encrypting the personal data using a second key associated with the second site; and computer code for transmitting the re-encrypted personal data to the second site via the network, wherein the second site decrypts the re-encrypted personal data with the second key and uses the personal data to complete the second portion of the transaction (In using the Internet to effect transactions, it is inherent for the terminal to decrypt the smartcard data in order to read it, and then to re-encrypt it using an encryption protocol that the destination would understand. A terminal would need to be able to read the information from the

smart card and would so decrypt it. In order to send the information over the Internet, it must be encrypted for security purposes).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 7 and 17 rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al.

As per claim 7:

Davis et al discloses:

- secure device provides the terminal with the encrypted personal data prior to and separately from the first key (providing the terminal with the encrypted information separately from the key (which is needed to decrypt the data) was well known to those skilled in the art at the time of the invention. Without the key, the data cannot be decrypted. If the key were provided inside the encrypted data, there would be no way to obtain either the key or the data. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the key separately from the personal information.)

As per claim 17:

Davis et al discloses:

- secure device provides the terminal with the encrypted personal data prior to and separately from the first key (providing the terminal with the encrypted information separately from the key (which is needed to decrypt the data) was well known to those skilled in the art at the time of the invention. Without the key, the data cannot be decrypted. If the key were provided inside the encrypted data, there would be no way to obtain either the key or the data. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the key separately from the personal information.)

Claims 2 and 13 rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al, in view of Official Notice.

As per claim 2:

Davis et al discloses:

- the secure device includes a special region that, if tampered with, renders the secure device inoperable and thereby prevent access to the first key contained therein (As shown above, Davis et al discloses that it aims to keep private information secure, using encryption on a smart card. It uses encryption techniques and a system to prevent leakage of personal information. Davis et al does not teach a device whereby any attempting tampering results in the device deactivating itself. The Examiner takes Official Notice that deactivating circuitry

upon an intrusion attempt was well known to those skilled in the art at the time of the invention. It has been well known to use a mechanism to destroy information, when an attempt to breach the security of the information is made (in order to prevent illicit retrieval of the data). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use a mechanism to deactivate or destroy the information in the card, upon an intrusion attempt.)

As per claim 13:

Davis et al discloses:

- the secure device includes a special region that, if tampered with, renders the secure device inoperable and thereby prevent access to the first key contained therein (As shown above, Davis et al discloses that it aims to keep private information secure, using encryption on a smart card. It uses encryption techniques and a system to prevent leakage of personal information. Davis et al does not teach a device whereby any attempting tampering results in the device deactivating itself. The Examiner takes Official Notice that deactivating circuitry upon an intrusion attempt was well known to those skilled in the art at the time of the invention. It has been well known to use a mechanism to destroy information, when an attempt to breach the security of the information is made (in order to prevent illicit retrieval of the data). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to

use a mechanism to deactivate or destroy the information in the card, upon an intrusion attempt.)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher C. Johns whose telephone number is 571-270-3462. The examiner can normally be reached on Monday-Thursday, 7:30-5, Alternate Fridays, 7:30-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tom Dixon can be reached on 571-272-6803. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher C Johns/
Examiner, Art Unit 4172

Christopher Johns
Examiner
Art Unit 4172

CCJ

/Naeem Haq/
Primary Examiner, Art Unit 4172